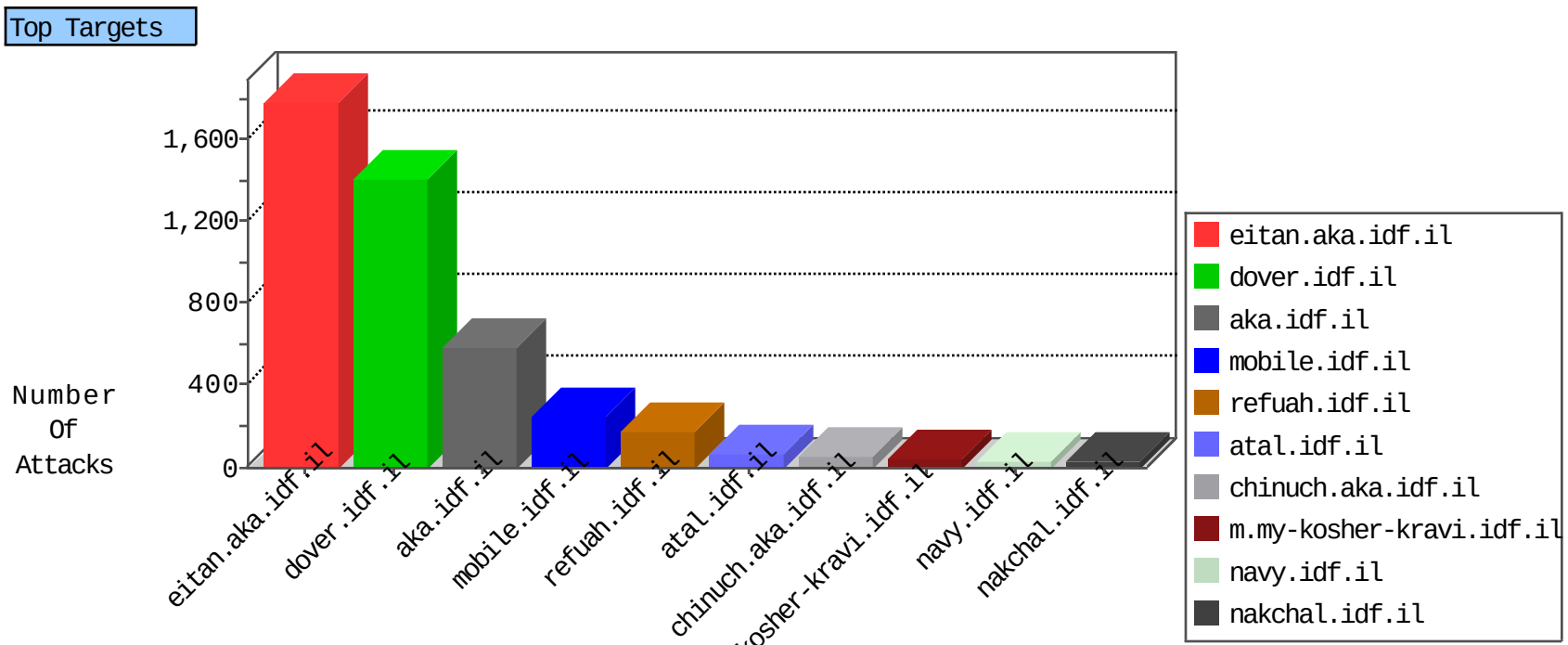
10-31-2015-11:04:02 to 10-31-2015-12:04:02

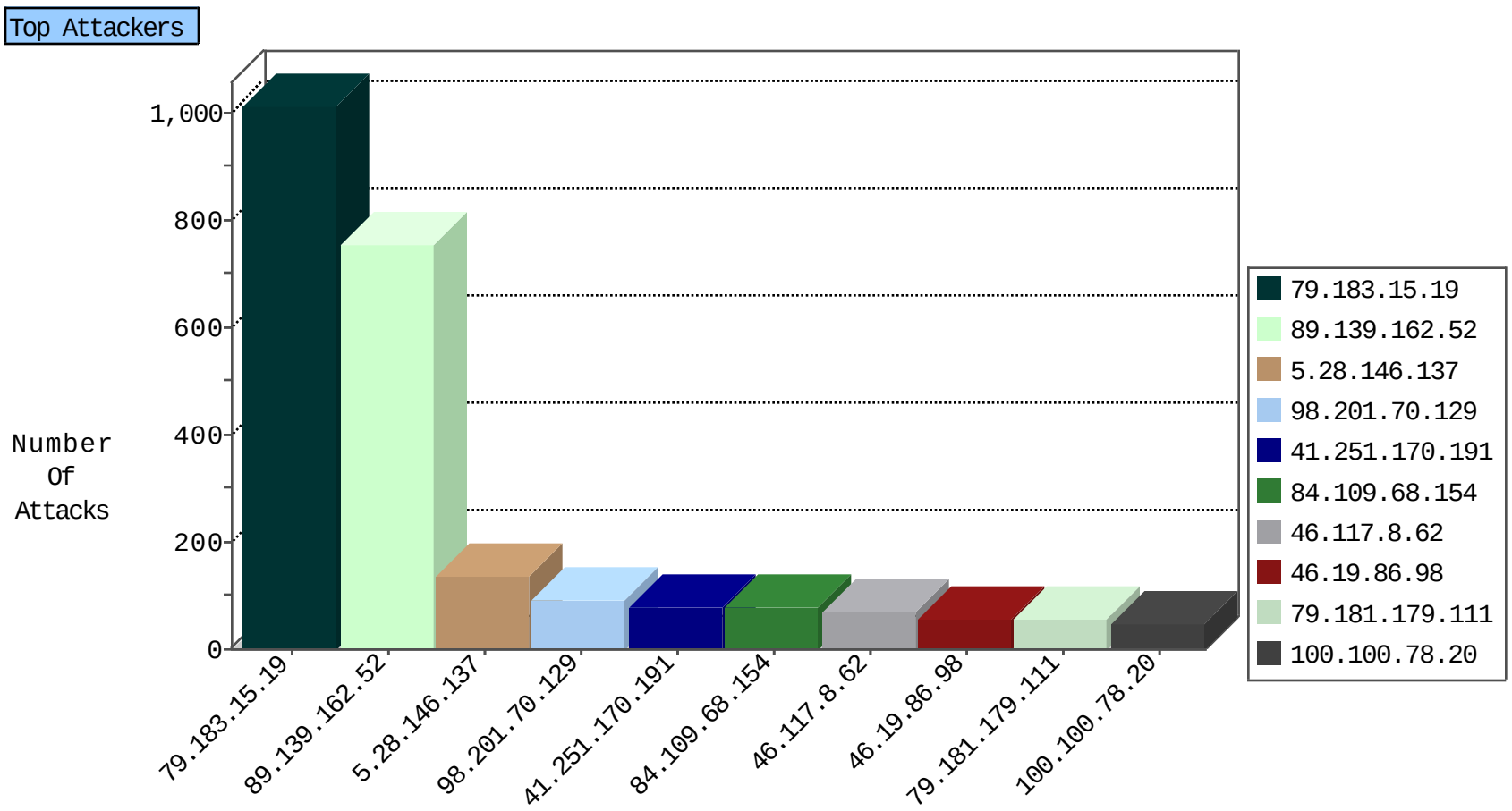
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-31-2015-11:04:02 to 10-31-2015-12:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	904
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	262
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	215
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	193
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	101
84.111.139.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	39
79.177.216.31	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
31.154.91.26	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
84.228.110.76	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
2.52.4.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
37.142.68.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
5.29.187.3	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
2.54.14.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
37.26.147.134	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
79.183.101.172	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
79.180.132.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
82.81.16.174	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
79.176.150.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
5.29.152.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
85.64.158.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.108.244.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
5.102.254.195	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.183.101.172	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
176.13.14.152	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.67.181.63	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.35.140	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.32.179.78	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.183.101.172	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
79.180.132.109	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
176.13.15.154	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.183.3.238	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.14.251	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.52.4.242	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
37.142.204.154	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.160.235.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.199.76.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.179.164.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.69.102.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.229	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
176.13.14.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.67.117.221	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
149.78.254.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
149.88.194.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
87.68.40.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.138.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.67.43.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.180.212.159	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.182.96.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
93.172.11.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

10-31-2015-11:04:02 to 10-31-2015-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.179.111	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9

10-31-2015-11:04:02 to 10-31-2015-12:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-31-2015-11:04:02 to 10-31-2015-12:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.15.19	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	444
98.201.70.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
41.251.170.191	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
213.175.183.170	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
79.176.39.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
100.100.118.248		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
46.19.86.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
100.100.78.20		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
100.100.78.20		147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	23
89.139.162.52	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
100.100.121.113		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
84.109.68.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
79.181.179.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
79.181.179.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	15
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
31.154.91.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.183.101.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.54.8.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.29.187.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.158.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.47.94		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.91.241		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.117.8.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
82.80.79.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
84.111.139.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
147.236.34.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.142.68.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.67.181.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.177.166.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.160.235.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.67.117.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.19.116.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.176.150.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.64.195.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.170.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.28.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.124.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.100.60.252		147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	6

10-31-2015-11:04:02 to 10-31-2015-12:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.162.52	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 89.139.162.52	Block	720
79.183.15.19	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	570
5.28.146.137	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.28.146.137	Block	105
46.117.8.62	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	60
84.109.68.154	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	60
217.132.222.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	30
87.69.167.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	30
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
5.28.146.137	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	30
40.77.167.44	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	30
46.116.190.74	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.116.190.74	None	15
87.68.21.133	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	15
5.102.254.209	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
207.46.13.155	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	15
77.125.141.250	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
176.12.145.119	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
46.19.85.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/17329.jpg	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.4	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	15
87.68.21.133	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method undefined in URL www.aka.idf.il/main/giyus/api/api/answers	Block	15
77.125.154.23	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	15
37.230.221.40	Russian Federation	147.237.72.166	aka.idf.il	Malformed URL main/home/default.aspx	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	15
176.13.18.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
93.172.142.250	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	15
79.183.54.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
46.19.86.98	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	15
5.28.129.132	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	15
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/size220x0/17344.jpg	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	15
66.249.78.27	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	15
157.55.39.122	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	15
79.178.116.232	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	15
37.230.221.40	Russian Federation	147.237.72.166	aka.idf.il	Multiple Malformed URL from 37.230.221.40	Block	15
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	15
180.76.15.163	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/clientscripts/mediagallery/{1}	Block	15
93.172.150.227	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	15
66.249.67.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	15
46.19.86.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	15
66.249.78.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	15
173.252.81.116	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/112536.pdf&ved=0cbkqfjaaahukewi1g6xz6eriahugvrqkhvy7abi&usg=afqjcnffmwdibxqfzjqb_0-lwusvxyh9ng	Block	15
46.121.214.103	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
89.139.5.120	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	15
79.181.122.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
40.77.167.0	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15

10-31-2015-11:04:02 to 10-31-2015-12:04:02